

kaspersky

Jak vzdělávat své zaměstnance na kybernetickou bezpečnost

Petr Kuboš | Enterprise Sales Manager CZ a SK

Fakta o Kaspersky

> 22

let historie

> 4,000

vysoce kvalifikovaných zaměstnanců

> 400,000,000

uživatelů celosvětově je chráněno našimi
technologemi

> 270,000

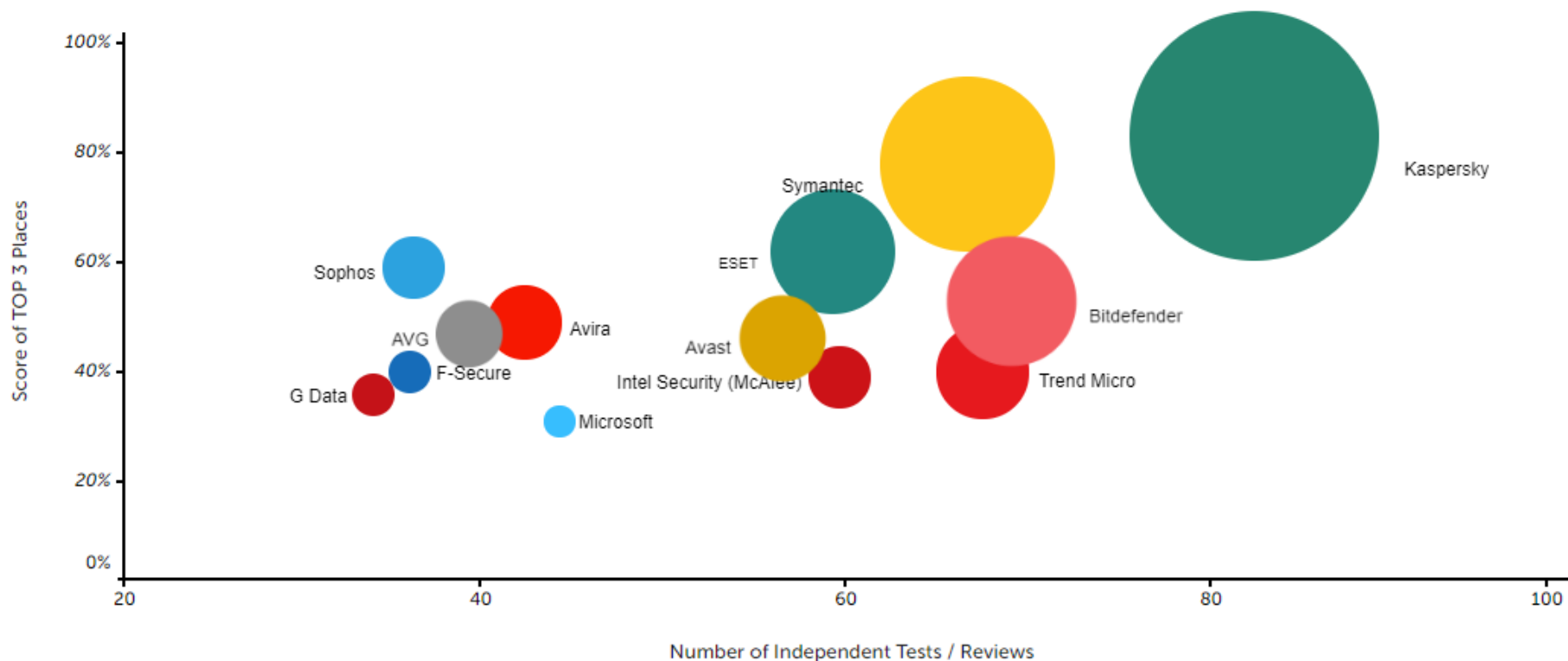
firemních zákazníků celosvětově

> Celosvětově největší, soukromě
vlastněná bezpečnostní společnost



Kaspersky ochrana – nejvíce testována, nejlépe oceňována.

V roce 2019 se produkty Kaspersky Lab zúčastnily 86 nezávislých testů a recenzí. V 64 případech obsadily první místo a v 81% skončily v první trojce.



<https://www.kaspersky.com/top3>



* Notes:

- According to summary results of independent tests in 2019 for corporate, consumer and mobile products.
- Summary includes independent tests conducted by: AV-Comparatives, AV-Test, SE Labs, MRG-Effitas, Virus Bulletin, ICSA Labs, PCSL, NSS Labs.
- Tests performed in these programs assess all protection technologies against known, unknown and advanced threats.
- The size of the bubble reflects the number of 1st places achieved.

Transparency – a new cybersecurity trend

Globálně propojený svět vyžaduje zvýšenou transparentnost. Společnost Kaspersky pokračuje ve vývoji své „Global Transparency Initiative“, jejímž cílem je prokázat náš trvalý závazek zajistit integritu a důvěryhodnost řešení společnosti ve službách našich zákazníků.

Data storage and processing

Ve švýcarských datových centrech jsme začali uchovávat veškerá data Evropských zákazníků a zpracovávat škodlivé a podezřelé soubory které s námi Kaspersky zákazníci sdílejí.

Transparentní centra

Otevřeli jsme transparency centra v Curychu, Švýcarsku a Madridu, Španělsku a v Kuala Lumpur. Čtvrté středisko transparentnosti v Brazílii bude otevřeno v průběhu roku 2020

Bug bounty program

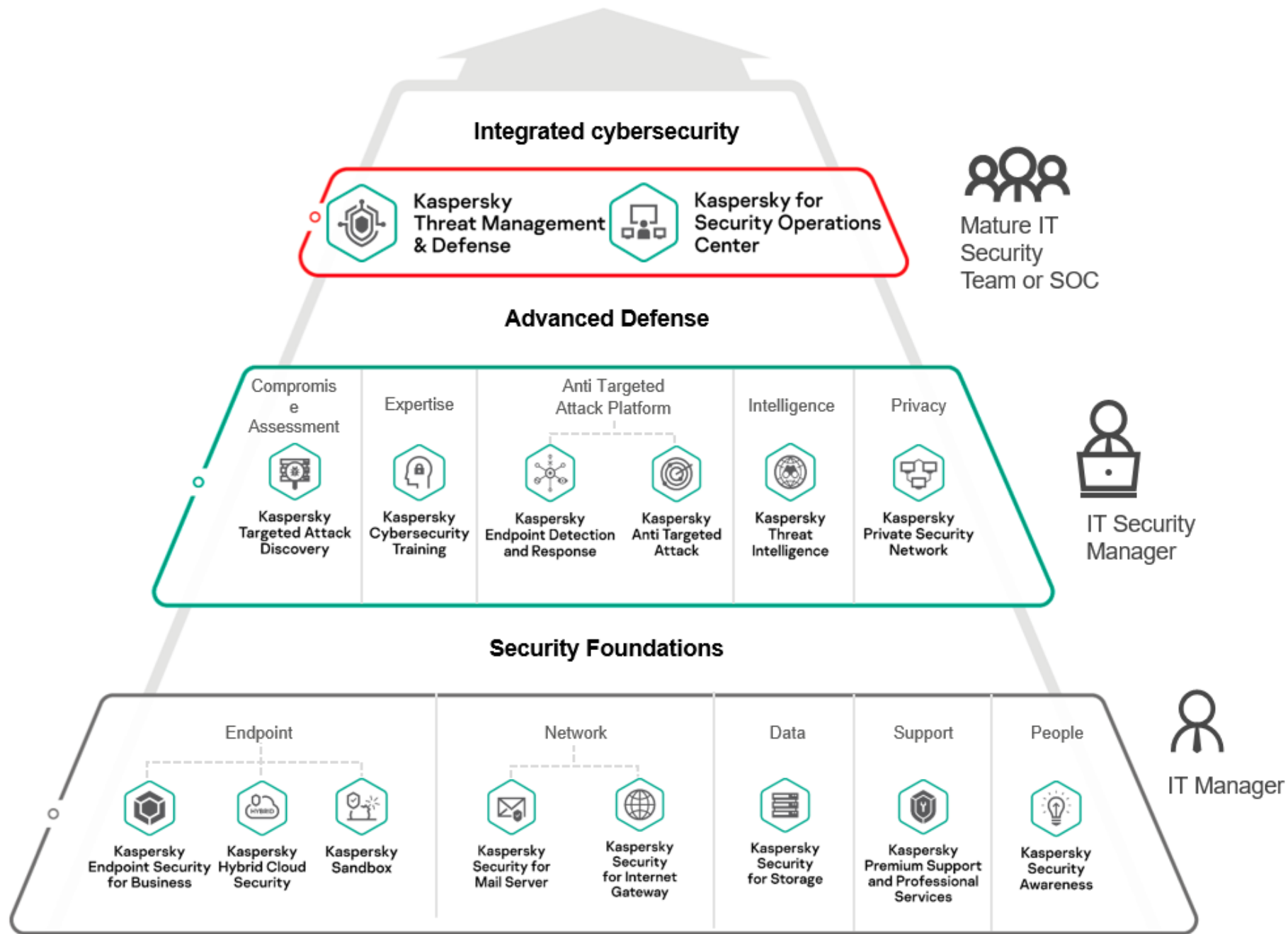
Zvýšili jsme odměny za nalezení chyb v produktech Kaspersky až na 100 000 \$ za objevenou zranitelnost





„Komise nedisponuje žádnými důkazy týkající se potenciálních problémů souvisejících s používáním produktů společnosti Kaspersky Lab.“

EU Commissioner for Digital Economy and Society



Vývoj malwaru

STUPNICE NÁRUSTU HROZEB

1994

1

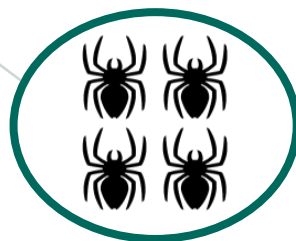
NOVÝ VIRUS
KAŽDOU
HODINU



2006

1

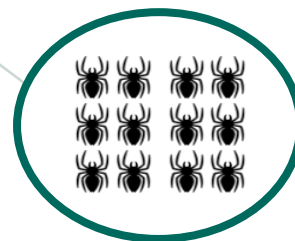
NOVÝ VIRUS
KAŽDOU
MINUTU



2011

1

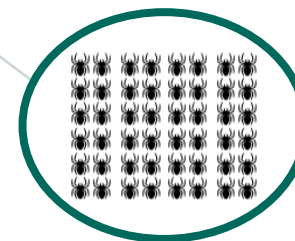
NOVÝ VIRUS
KAŽDOU
SEKUNDU



2014 - 2019

+300,000

NOVÝCH
VZORKŮ
KAŽDÝ DEN



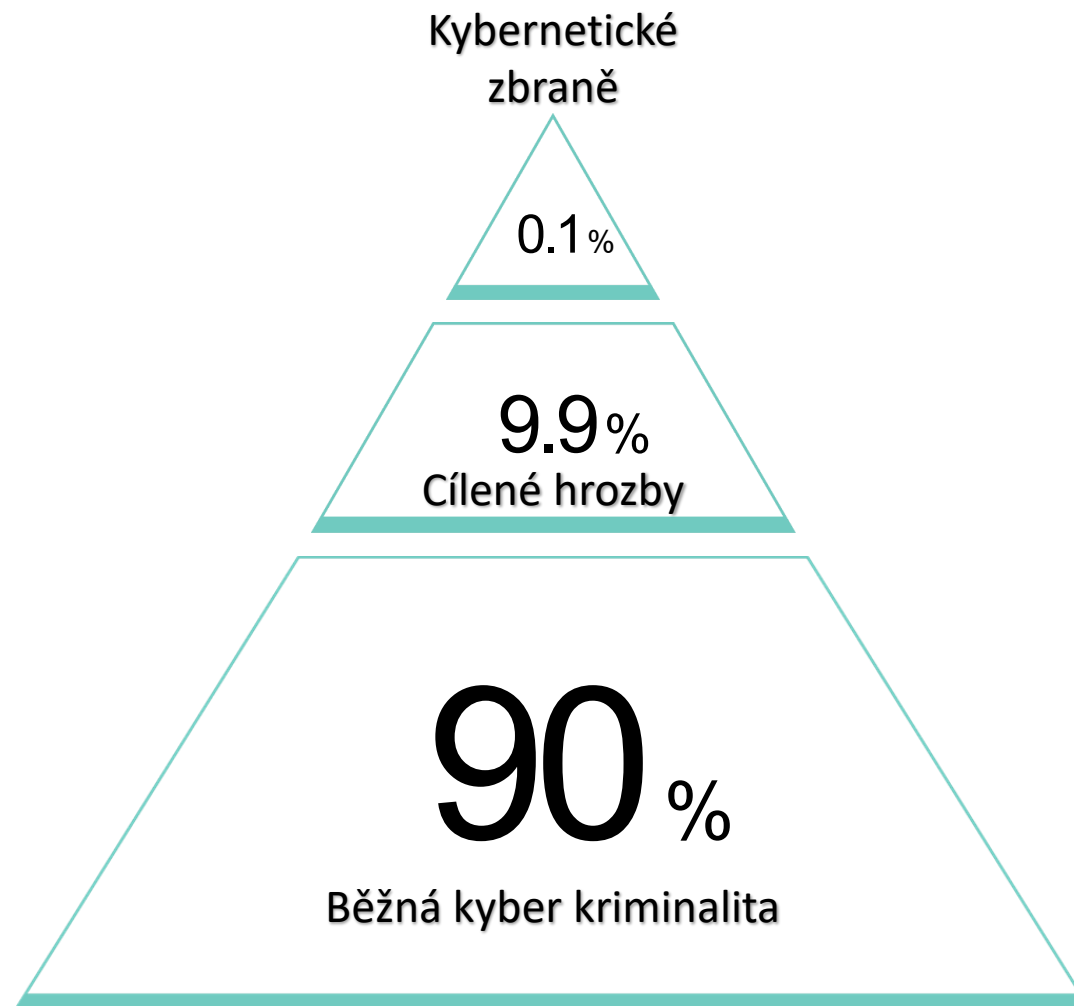
+360,000

Kaspersky detekuje více než 360,000 nových
unikátních

škodlivých vzorků, denně.

Skladba kybernetických hrozeb

kaspersky



APT – pokročilé persistentní hrozby a útoky,

Cílené útoky a pokročilý malware

„běžné“ hrozby



Profi IT Security Team or SOC



IT Security Manager



IT Manager

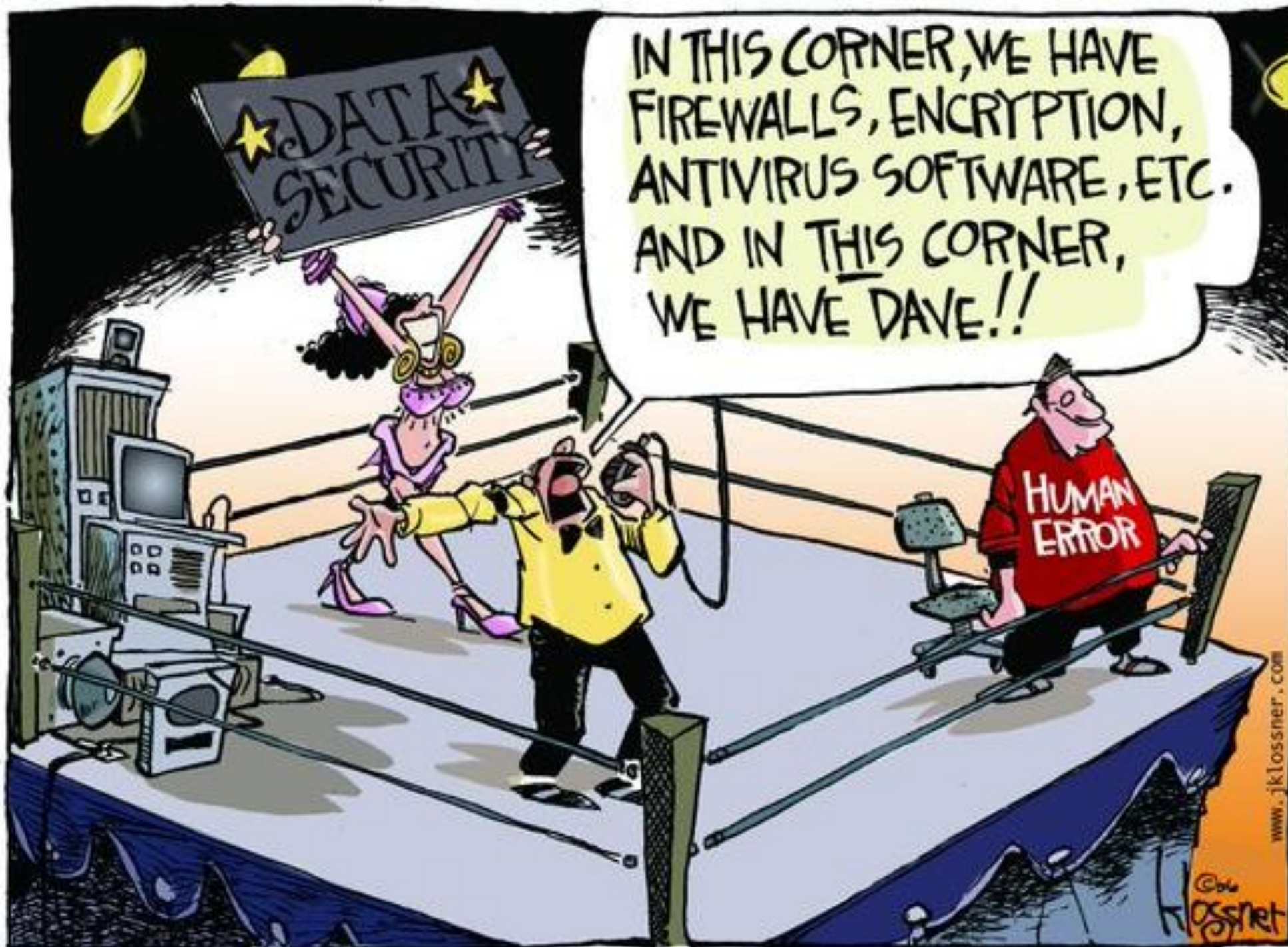
Kybernetické hrozby

jsou realitou dnešních dnů.

Hlavní rizika obchodních společností v roce 2018



2018



IN THIS CORNER, WE HAVE
FIREWALLS, ENCRYPTION,
ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER,
WE HAVE DAVE!!

www.jklossner.com

copyright 2006 john klossner, www.jklossner.com

John Klossner

kaspersky

SECURITY TODAY



UŽIVATELÉ JSOU TEN NEJSLABŠÍ ČLÁNEK



Až **80%** všech kybernetických incidentů jsou způsobeny lidskými chybami.
Společnosti utrácejí miliony za jejich nápravu.

Lidský faktor jako významná bezpečnostní hrozba

Chování zaměstnanců je pro organizace významná IT bezpečnostní hrozba, navzdory tomu, že jsou využívány tradiční způsoby školení zaměstnanců.



\$1,057,000

v Enterprise organizaci

Průměrný finanční dopad způsobený únikem dat a kybernetickými incidenty zaměstnanců či nedostatečnými IT zdroji



\$98,000

v SMB

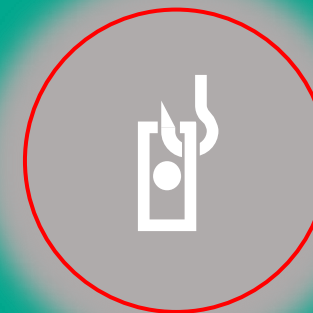
Průměrný finanční dopad způsobený únikem dat a kybernetickými incidenty zaměstnanců či nedostatečnými IT zdroji



\$101,000

v SMB

Finanční dopad útoků způsobených phishingem. *



up to **\$400**

na zaměstnance a rok

Průměrné náklady na řešení phishingového útoku

Proč je důležité vybrat si ten správný vzdělávací program?

Nezajímavé a neefektivní pro zaměstnance:



Považován za obtížné, nudné, nedůležité.



Většinou je to o : „co nesmíte“ než „jak na to“



Účastníci si po školení nic nepamatují



Čtení a poslouchání není efektivní



Přítěž pro administrátory:

Jak vytvořit vzdělávací program a nastavit cíle školení?



Jak zvládnout proces vzdělávání?



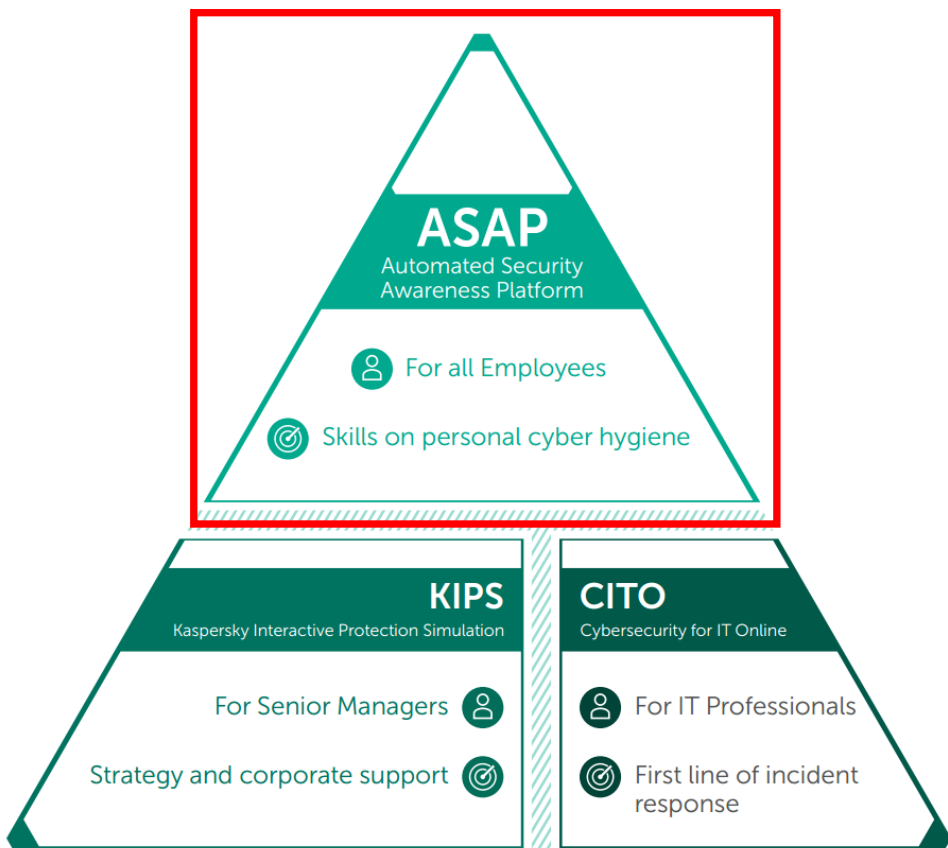
Jak kontrolovat průběžné výsledky?



Jak oslovit zaměstnance aby se zapojili do školení



Kaspersky vzdělávací programy kybernetické bezpečnosti



Praktické dovednosti místo jen znalostí

PC orientované, jednoduché na správu a doručení, skvělý reporting.

Příklady z reálného světa & praktické cvičení – zaměstnanci jsou motivováni a zapojeni do vzdělávacího programu

Jednoduchá správa pro administrátory a efektivní pro organizaci

Redukuje počet lidských chyb a selhání až o

80%

01

Kaspersky Automated Security Awareness Training

02

An easy-to-manage online tool which builds employee's cybersecurity skills level by level

03

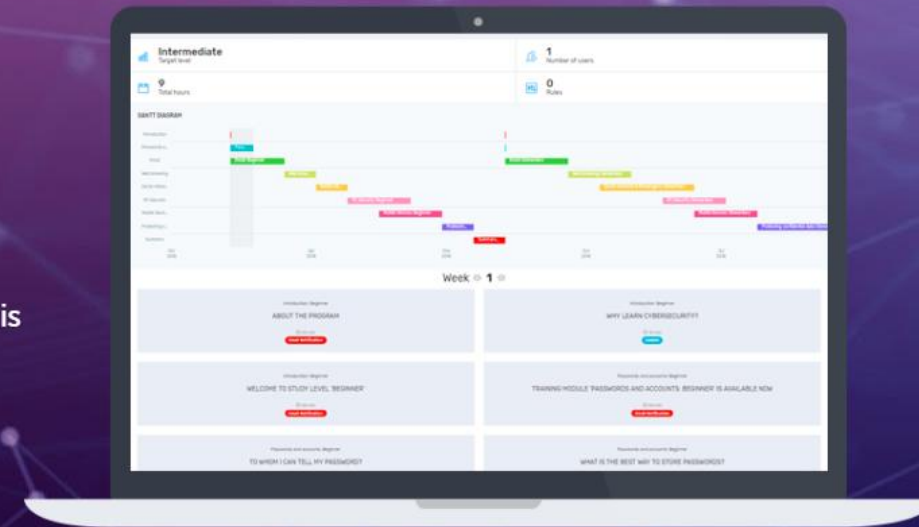
Kaspersky Automated Security Awareness Platform (ASAP) is created by leading cybersecurity experts to protect your business

04

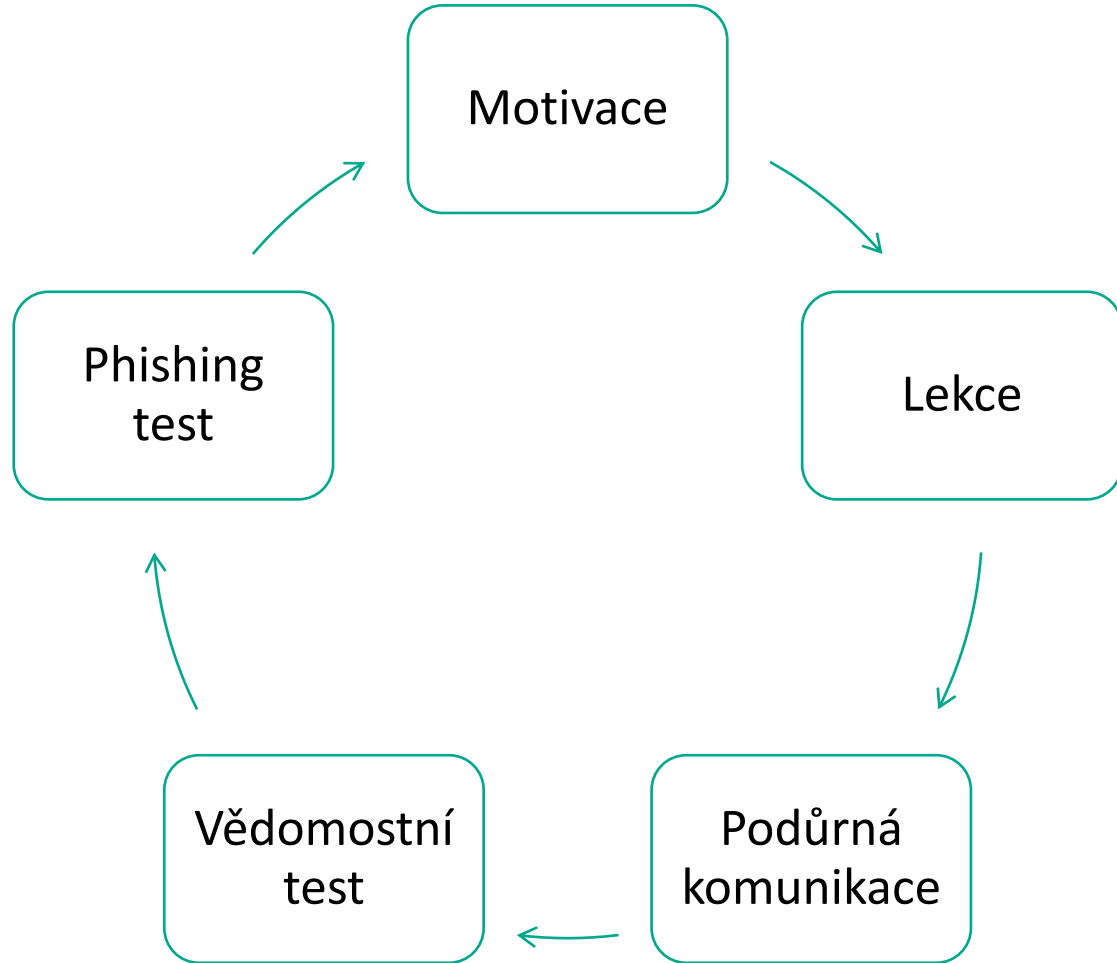
Launch your awareness program online in just a few steps

[TRY NOW >](#)

05

[View Datasheet](#)[View Demo](#)

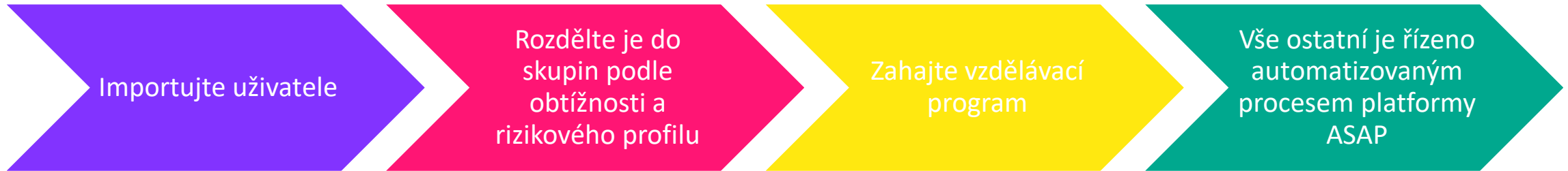
Automatizovaná vzdělávací platforma



- Všechny typy vzdělávacích modulů jsou automaticky naplánovány a automaticky přiřazeny uživatelům.
- Vzdělávací cyklus se opakuje v průběhu délky licenčních podmínek
- Témata jsou logická a časově nezaťěžují studující uživatele.

Plně automatizovaná podpora a správa vzdělávací platformy

Jak začít vzdělávat své zaměstnance?



Pouze tento krok vyžaduje vaši úvahu a rozhodnutí o rozdělení do profilů

Vše ostatní, jako:

- Individuální plánování programu
- Individuální týdenní reporty pro zaměstnance
- Pravidelné reporty pro administrátory

Budou provedeny automaticky bez zásahu administrátora.

Jednoduchý ovládací panel - vše na jednom místě...

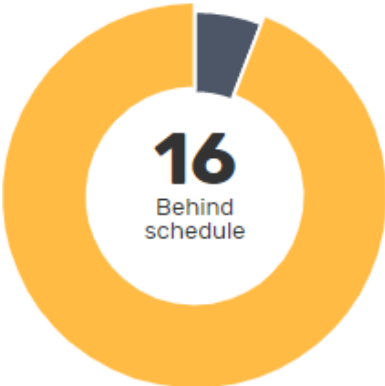
BĚŽNÉ ÚKOLY

MY ACTIONS

- Add new users
- Import Users
- Start Group Training
- Add to training
- Pause Training
- Resume Training
- Download report

STUDENTI POTŘEBUJÍCÍ POMOC

WHO NEEDS MY ATTENTION?



16
Behind schedule

Can not finish on time	1
Significantly behind schedule	0
Behind schedule	16
Going well	0
Ahead of schedule	0

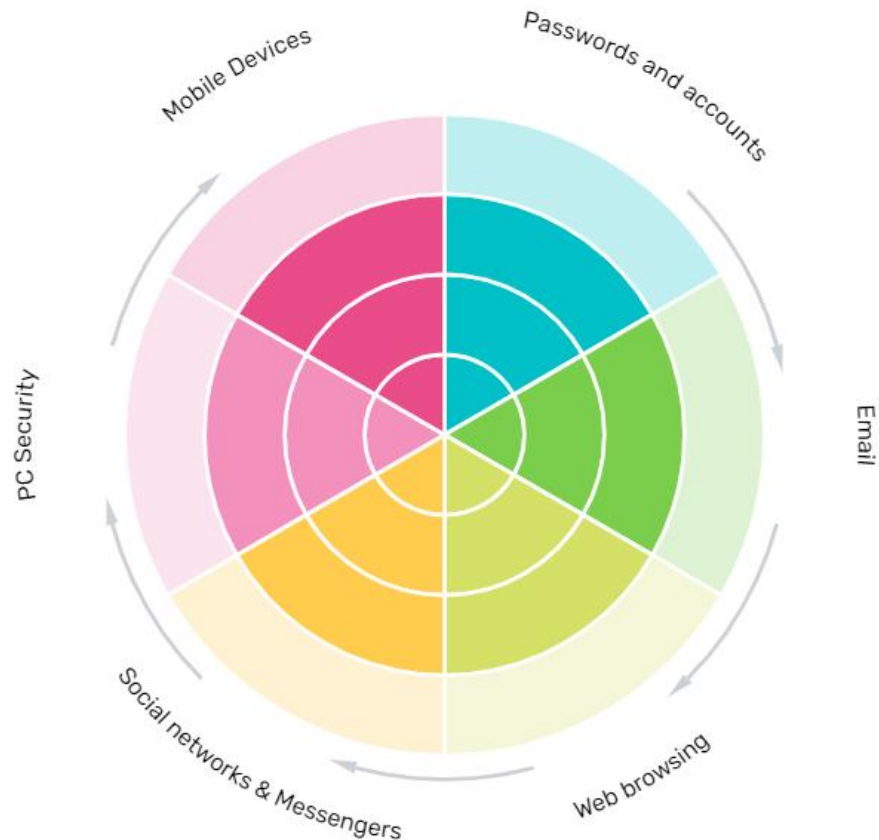
PŘEHLED LICENCÍ

USERS & LICENSES

Studying	14
Completed	0
Unassigned	130
Paused	3
Total users	147

10 Total number of available licenses	30 Total number of licenses
---	---------------------------------------

Automatizovaná vzdělávací platforma (ASAP)



Více než 350 lekcí strukturovaných do 3 úrovní obtížnosti a 6 témat

- Hesla a účty
- Email
- Web browsing
- Social networks & messengers
- PC Security
- Mobile devices

+ Různé druhy vzorů phishingových emailů

Dostupné v 10 jazycích

CZ a SK verze – červen 2020

Report pouze 1 kliknutím

Report si můžete stáhnout pouze 1 kliknutím.

USERS' PERFORMANCE REPORT EXAMPLE

Total users	1500		
Study status for each one:			
Unassigned	17		
Studying	1483		
Paused	0		
Completed	0		
Archived	0		
Licenses in Use	1483		
Who needs my attention?			
Study Speed	Number of Users	Reasons For Falling Behind	Number of Users
Total Studying	1483		
Ahead of schedule	31		
Going well	1386		
Behind schedule	58	Do not take tests	3
		Fail tests	55
		Never entered the platform	0
Significantly behind schedule	8	Do not take tests	6
		Fail tests	2
		Never entered the platform	0
Can not finish on time	0	Do not take tests	0
		Fail tests	0

PLATFORM INTERFACE EXAMPLE

MY ACTIONS ?

Add new users

Import Users

Start Group Training

Add to training

Pause Training

Resume Training

Download report

Uživatelské rozhraní - náhled

The screenshot displays the user interface of the Kaspersky Automated Security Awareness Platform. The top navigation bar includes 'Course History' and 'My achievements'. The user's name 'Petr' and language 'English' are visible in the top right corner.

Dear Petr,
You are in the active phase of the training.
You have lessons or tests available! Complete them to find out more about cybersecurity!

Your group: **Low Risk** (6 training units)

PASSWORDS AND ACCOUNTS: BEGINNER Start

Approximately 90% of passwords are vulnerable to hacking. Many people use simple passwords, assuming that no one is going to try to access their account, but they're wrong. Any account can be hacked, even if its owner thinks that it is not valuable enough to be a target.
Once an attacker has your password, he can borrow money from your friends in your name, send malware to your contacts, publish something dubious on your page, or even withdraw money from your bank account. So it's important to know how to use passwords properly.

Why don't people worry about the security of their passwords and the kinds of errors that slip through? Lesson 1-2 min Repeat

Can I tell my passwords to others? Lesson 2-4 min Repeat

How do I safely store passwords? Lesson 4-8 min Repeat

Your Progress
4%

Planned end date: 05/12/2019
Estimated end date: 08/18/2020
Cannot finish on time

Knowledge test for module 'Passwords and accounts: Beginner' Knowledge Test 10-20 min Start

EMAIL: BEGINNER Start

Email is the main channel of corporate communication. Nearly every Internet user has an email account, and as a rule, they use it to create accounts with other services. If your email account is compromised, the attacker will gain access to your work email or bank information. Emails from cybercriminals can contain files and/or links that can harm you and your organization.
Learn the basic rules of cybersecurity to avoid becoming a victim of these cyberattackers.

WEB BROWSING: BEGINNER Start

Statistics indicate that a cybercrime occurs somewhere in the world every 10 seconds. Their consequences can be truly grievous, ranging from loss of personal data to blackmail, or from incessant ads to outright theft of money. You can fall victim to such attacks by opening an executable file containing malware, following a dangerous link, entering your data on a fake page, etc. That is why every Internet user should have certain basic skills they can use to protect themselves, and their company, from would-be cybercriminals.

SOCIAL NETWORKS & MESSENGERS: BEGINNER Start

ASAP obchodní model

- License začínající od 5 uživatelů
- Cena za 1 rok / 1 uživatel, podle celkového počtu uživatelů
- Spravujte více společností pod jedním účtem
- Online web verze – v přípravě SCORM offline verze
- Zkouška na období 2 měsíců pro 3 uživatele, zdarma
- Demo [interaktivního modulu](#)

01

Kaspersky Automated Security Awareness Training

02

An easy-to-manage online tool which builds employee's cybersecurity skills level by level

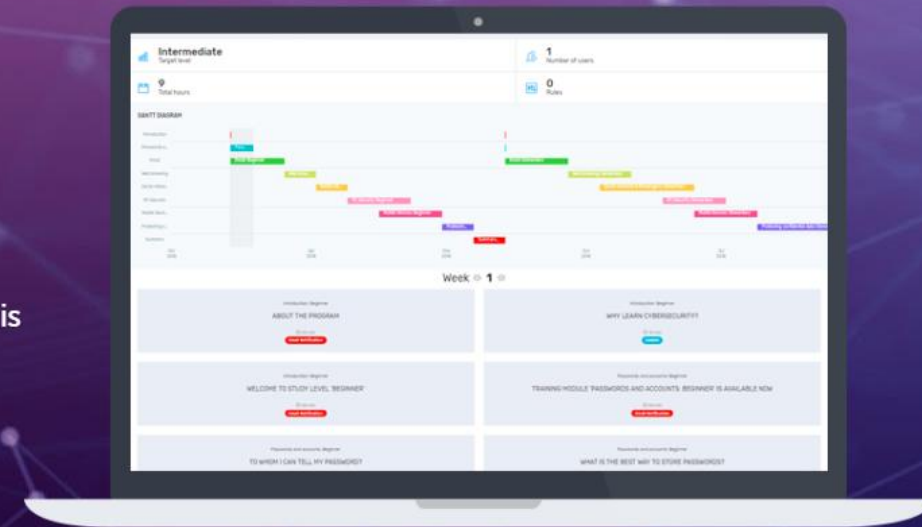
03

Kaspersky Automated Security Awareness Platform (ASAP) is created by leading cybersecurity experts to protect your business

04

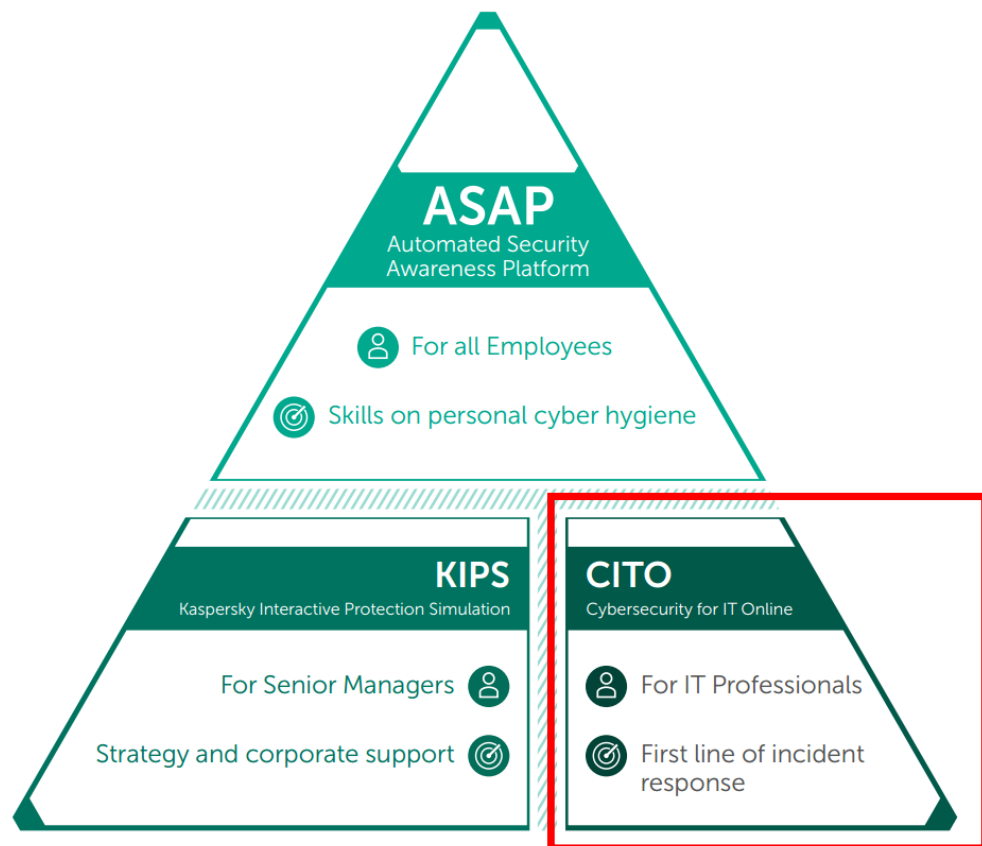
Launch your awareness program online in just a few steps

05

[TRY NOW >](#)[View Datasheet](#)[View Demo](#)



Kaspersky Security Awareness - CITO



Cyber Security for IT Online
Efektivní školení pro všechny
IT specialisty

Snižuje
počet lidských chyb
až o:

80%

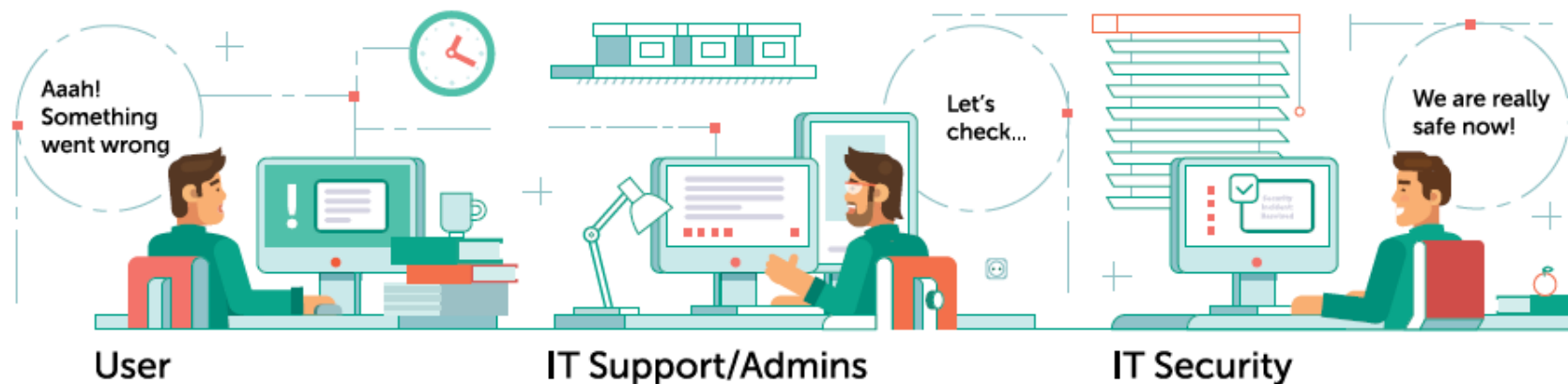
<https://cito.cloudapp.net/>

IT specialisté – Nové role a odpovědnosti – dříve a nyní

Now



Should be



Cybersecurity For IT Online

Cíle vzdělávání ?

- Kritické myšlení o bezpečnosti v IT
- Znalost hackerských nástrojů a technik
- Základní dovednosti analýzy hrozeb
- Znalosti, jak pomoci bezpečnostnímu oddělení při reakci na incident

Pro koho je určeno ?

- Service desk
- IT / síťoví profesionálové
- IT bezpečnost
- Místní správci a další technicky pokročilí zaměstnanci

4 moduly, ~ 30 praktických cvičení

Malicious Software

Verification of existence or absence of incident related to malware

#Processhacker, #Autoruns, #Fiddler,
#GMER

Potential unwanted Programs

Working with event monitors of the systems and sandboxes. Using statistical engines (virustotal). Removing PuPs

#ProcessMonitor, #Cuckoo, #Virustotal

Phishing Incident Response

Phishing emails lookup. Verification of the incident related to phishing. OSINT

#ExchangeComplianceSearch , #Robtex,
#Whois, #GoogleDorks

Investigation Basics

Incident localization, data collection, collecting digital evidence, log and timeline analysis

#EventLogExplorer, #Autopsy, #FTK-Imager

Cybersecurity For IT Online

Awareness => incident response training

The screenshot displays a training interface for Malware Hunting. On the left, a sidebar titled 'BASIC HEURISTICS' provides instructions for the exercise. The main area shows a remote administration session for IP 192.168.152.2, with Process Hacker 2 open. The Process Hacker window shows a list of processes with columns for Name, PID, CPU, I/O T..., Privat..., User..., Description, Verified Signer, and Verificat... The task scheduler process (taskhost.exe) is highlighted in blue.

BASIC HEURISTICS

In first exercise we will explore Process Hacker

Launch Process Hacker and find abnormal and suspicious process, which does not contain any information in the Description column

Some system processes also do not have Description – it's OK.

If you want to repeat the theoretical part, [click here](#)

Analyze the list of processes using the Process Hacker and enter the answer below

Enter the PID of the process without description:

Enter suspicious process PID:

192.168.152.2 - Remote Administration

Process Hacker 2

Name	PID	CPU	I/O T...	Privat...	User ...	Description	Verified Signer	Verificat...
winlogon.exe	468			19.9 KB	NT AU...	Windows Logon Ap...	Microsoft Windows	Trusted
wininit.exe	404			41.9 KB	NT AU...	Windows Start-Up ...	Microsoft Windows	Trusted
services.exe	504			200.2 ...	NT AU...	Services and Contro...	Microsoft Windows	Trusted
svchost...	628			34.2 KB	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
task...	1792			52.5 KB	WIN-6...	Task Scheduler Engi...	Microsoft Windows	Trusted
Wmi...	3580			282.6 ...	NT AU...	WMI Provider Host	Microsoft Windows	Trusted
lsass.exe	692			42.7 KB	NT AU...	Local Session Mana...	Microsoft Windows	Trusted
sppsvc...	724			220.3 ...	NT AU...	Microsoft Software ...	Microsoft Windows	Trusted
dllhost...	772			114.5 ...	NT AU...	COM Surrogate	Microsoft Windows	Trusted
svchost...	864			1.2 MB	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
dllho...	1544			39.9 KB	WIN-6...	COM Surrogate	Microsoft Windows	Trusted
svchost...	904	0.1		322.4 ...	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
svchost...	1008	0.1		94.6 KB	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
svchost...	1076			508.4 ...	NT AU...	Host Process for Wi...	Microsoft Windows	Trusted
spoolsv...	1224			225.7 ...	NT AU...	Spooler SubSystem...	Microsoft Windows	Trusted

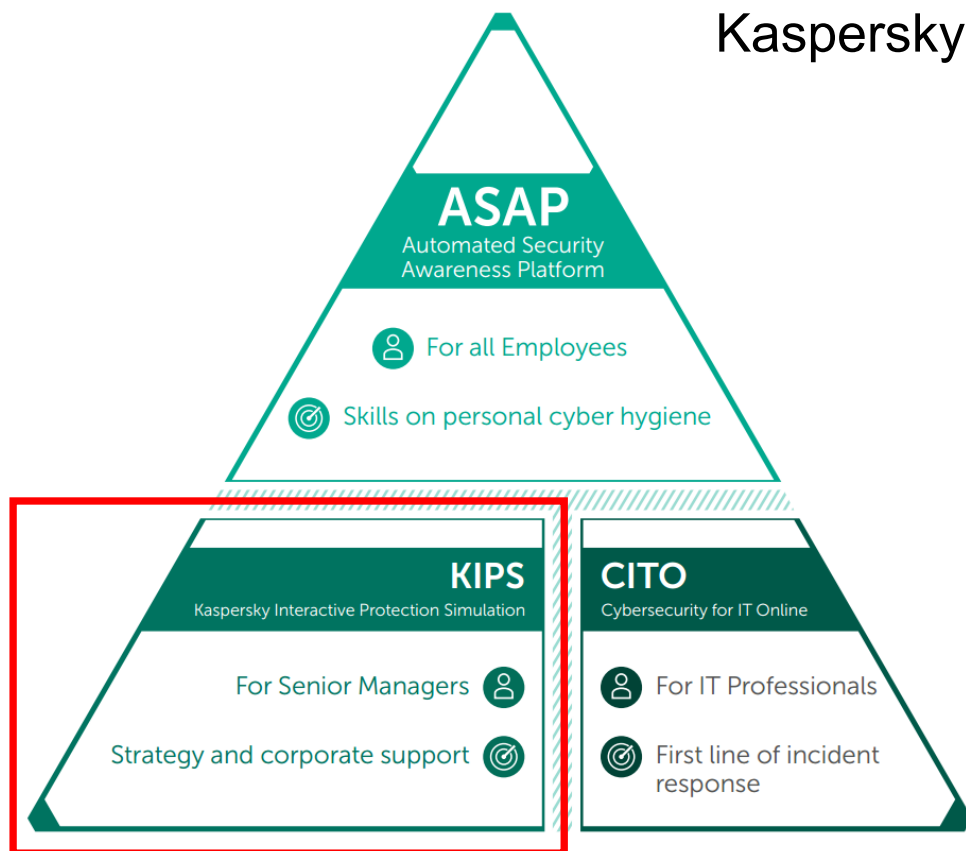
Cíle školení:

- Posílit „první linii obrany“ v reakci na kybernetické incidenty
- Snížit počet incidentů způsobených chybnou konfigurací
- Rozvíjet kritické myšlení týmů IT o kybernetické bezpečnosti



Kaspersky Security Awareness - KIPS

Kaspersky Interactive Protection Simulation



Snižuje
počet lidských chyb až o:

80%

Cybersecurity today – lost in a ‘corporate bermuda triangle’



CEO

Does not see how cybersecurity spendings relate to Revenues



SECURITY

Focus on protecting the confidential information
Many security controls are under IT management

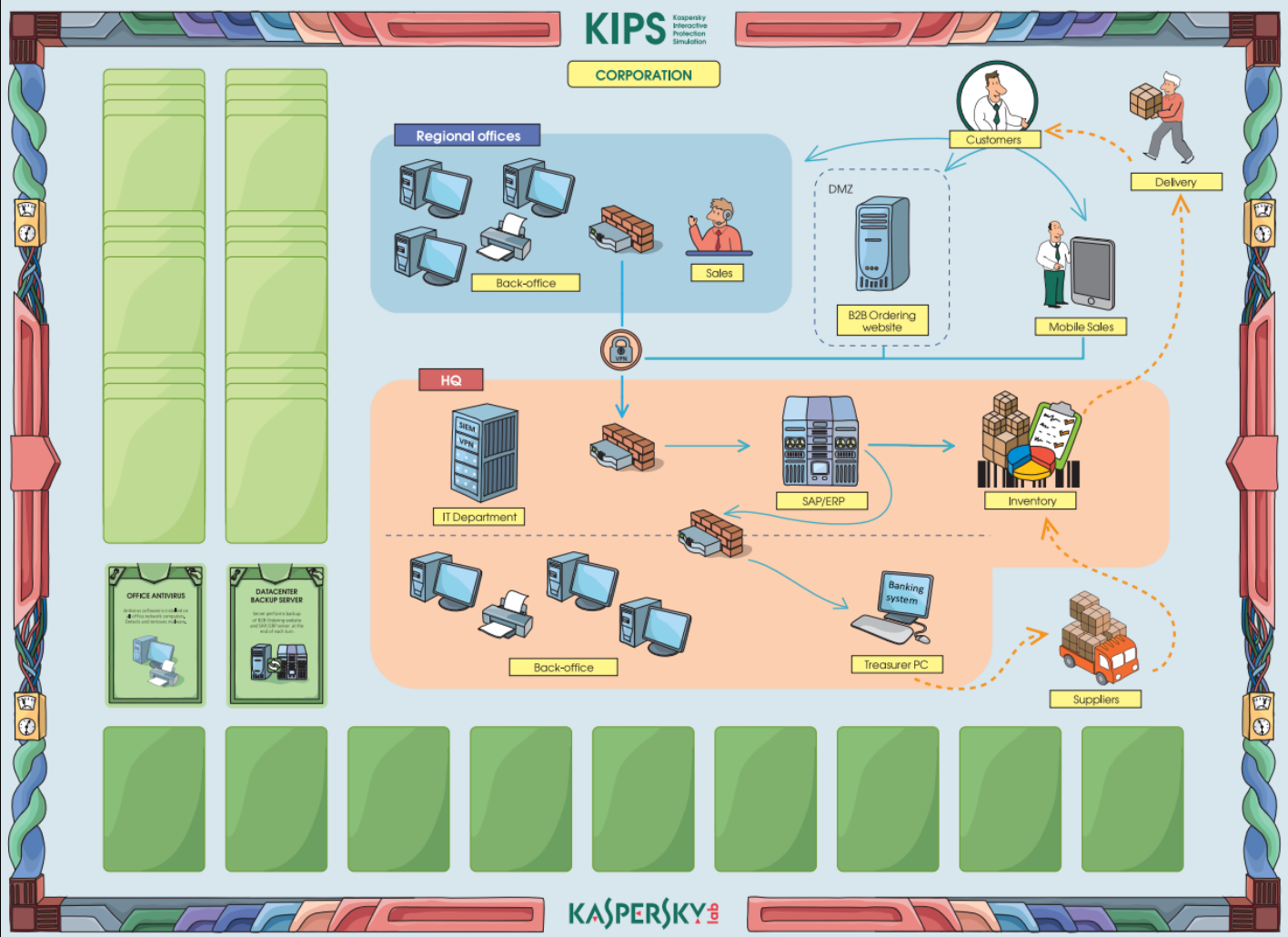


IT & BUSINESS MANAGERS

Focused on business efficiency, automation, new technologies

Mutual understanding and daily attention to cyberthreats between these 3 are crucial to successful cybersecurity in the modern business

KASPERSKY INTERACTIVE PROTECTION SIMULATION



Game Board



Web Console



Action Cards

KASPERSKY INTERACTIVE PROTECTION SIMULATION

- Senior managers

For IT, Business and Security – strategy simulation for cybersecurity decision-makers.

● Fun, engaging and fast (2 hours)

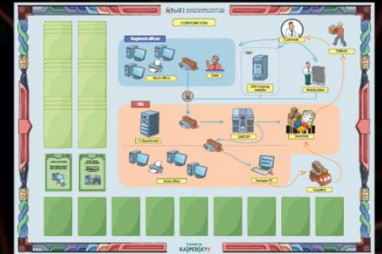
● Team-work builds cross-divisional co-operation

● Competition fosters initiative & analysis skills

● Gameplay develops an understanding of cybersecurity measures and strategy

● Teams compete at running a simulated enterprise and earning money

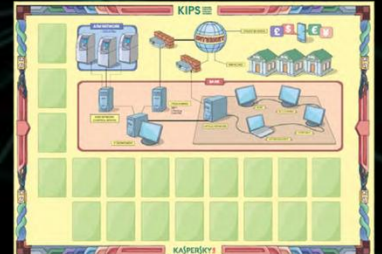
Corporate



Industrial



Financial



Government



KIPS Kaspersky
Interactive
Protection
Simulation

KASPERSKY

Training process overview

Game rules and housekeeping explained

Trainer tells about the game and its rules, trainees listen and follow slides on a big screen.

20 minutes

KIPS is played by teams

Players read news and decide on actions by choosing cards according to their strategy and budget and time limitations.

After each turn a rating is updated.

Trainer facilitates, encourages and controls timing.

40 - 50 minutes

Ideal scenario unveiled and lessons learned

Trainer tells about threats met by players, unveils the ideal scenario and draw participants to conclusions and practical takeaways.

20 - 30 minutes

Results announced – congratulations to winners!

Participants can be invited to share results and photos on social media.

10 - 20 minutes

Overall 1,5 – 2 hours

VYZKOUŠEJTE TO S NÁMI....



ComputerWeekly

"The Kaspersky Interactive Protection Simulation was a real eyeopener and should be made mandatory for all security professionals."

www.computerweekly.com/feature/Interactive-cyber-attack-a-dangerous-game



KASPERSKY

kaspersky

Děkuji Vám !